2006 CCRTS
The State of the Art and the State of the Practice

Perspectives on Information & Communications Technology (ICT) for Civil-Military Coordination in Crises

Gerard Christman
Office of the Assistant Secretary of Defense for Networks and Information Integration,
Directorate for Contingency Support and Migration Planning
6000 Defense Pentagon, Washington D.C. 20301-6000
Gerard.Christman.CTR@osd.mil
Franklin Kramer, Stuart Starr, Larry Wentz
National Defense University, Center for Technology and National Security Policy
Fort Lesley J. McNair, Washington D.C. 20319-5066
<kramerf><starrs><wentzl>@ndu.edu

Abstract

Nations all over the globe are confronting crises that demand enhanced coordination and information sharing between the responding civilian and military communities. These crises are generally divided into the categories of humanitarian assistance and disaster relief (HADR), stabilization and reconstruction (S&R), and complex emergencies. Although these types of crises can differ in their causes and specific impacts, there are significant similarities in the information and communications technology (ICT) to enable each of them.

The Directorate for Contingency Support and Migration Planning (CSMP), Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)), and the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), established a partnership that focused on identifying civil-military information sharing needs and commercial ICT capabilities supporting recent crisis operations. One of the major products from this partnership is a Primer designed to identify current knowledge and best practices in creating a collaborative civil-military information environment. This paper summarizes the major insights that have been developed in creating the Primer.

Introduction

Recently, the U.S. and other nations around the world have confronted a number of crises that demanded enhanced coordination and information sharing between the responding civilian and military elements. These crises are generally divided into the following three categories:

Humanitarian Assistance and Disaster Relief (HADR) is aid to an affected population that seeks, as its primary purpose, to save lives and alleviate suffering

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Perspectives on Information & Communications Technology (ICT) for Civil-Military Coordination in Crises	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Asst Sec of Defense for Networks and Information Integration,Directorate for Contingency Support and Migration Planning,6000 Defense pentagon,Washington,DC,20301-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**35**	

of a crisis-affected population. Humanitarian assistance must be provided in accordance with the basic humanitarian principles of humanity, impartiality and neutrality. These operations generally follow rapid-onset natural or man-made disasters. Humanitarian assistance provided by U.S. forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance (US JP 1-02). Recent examples include the Indian Ocean Tsunami, the hurricanes that battered the Gulf States of the U.S., and the earthquake in Kashmir.

Stabilization and reconstruction (S&R) efforts often work in tandem with peacekeeping operations and are designed to stabilize and regenerate political and economic development in the aftermath of a conflict. Notable examples include on-going operations in Afghanistan and Iraq.

A *complex emergency*, as defined by the UN Inter-Agency Standing Committee (IASC), is "a humanitarian crisis in a country, region or society where there is total or considerable breakdown of authority resulting from internal or external conflict and which requires an international response that goes beyond the mandate or capacity of any single and/or ongoing UN country program." Contemporary examples include the emergencies in countries such as Liberia and Haiti.

Although these types of crises can differ in their causes and specific impacts, there are significant similarities in the information and communications technology (ICT) needed to address all of them. In fact, the global revolution in commercial ICT has contributed many invaluable tools and removed many barriers to technical interoperability. As a result, a technical means exists to more easily create a collaborative civil-military information environment for coordination in crisis. This paper emphasizes the technical opportunities to improve the ICT support to forward deployed civil-military responders and improve the means to facilitate collaboration and information sharing among the participants on the ground and those supporting them. Although it is beyond the scope of this paper, it must be emphasized that there are institutional, cultural and social barriers that impede the building of trust among the participants in a crisis. These barriers serve to erode effective and timely collaboration. Thus, a complete solution to the problem of collaboration must address both technical and trust issues.

Over the last several years, the Department of Defense (DoD) has become increasingly interested in the challenges associated with responding to crises and the means for improving coordination and information sharing among the civil-military participants (references 1 and 2). The Directorate for Contingency Support and Migration Planning (CSMP), in the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)) and the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), established a partnership

that focused on identifying civil-military information sharing needs and commercial ICT capabilities supporting recent crisis operations.

A series of workshops and interviews with key civil-military organization participants were held during 2005 to capture insights and help frame the content for one of the major products from this partnership—a Primer designed to identify current knowledge and best practices in creating a collaborative civil-military information environment. The NDU Press is publishing the Primer. It is envisioned that the Primer will be a "living document" that will help all members of the civil-military community acquire and employ ICT to enable them to work collaboratively and share information to address future crises. This paper highlights some of the study findings that address ICT systems, data, best practices and the challenges related to achieving a civil-military information environment to facilitate collaboration and information sharing.

Nature of the Challenge

Civil-military coordination is of critical importance in both the planning and execution of crisis response, whether the risk stems from a potential hurricane or a "failed state." Critical areas for civil-military coordination are security (including rule of law), essential services (food, water, power, sanitation, medical, and shelter), logistics, communications, transportation and information.

The components of civil-military coordination consist of information sharing, task sharing and joint planning – all of which are dependent on communications and management of data and information. The following issues, however, often complicate effective civilian-military coordination:

- A lack of understanding about the information culture of the affected nation;
- Suspicions regarding the balance between information sharing and intelligence gathering;
- Tensions between military needs for classification (operational security) versus the civilian need for transparency;
- Differences in the command and control style of military operations versus less structured civilian activities; and
- The compatibility and interoperability of planning tools, processes and civil-military organization cultures.

The sharing of information is particularly critical because no single responding entity can be the source of all of the necessary information. Making critical information widely available to the civilian and military elements responding not only reduces duplication of effort, but also enhances coordination and provides a common knowledge base so that critical information can be pooled, analyzed, compared, contrasted, validated and reconciled. Civil-military collaboration networks for supporting responses need to be designed to dismantle traditional institutional "stovepipes," to facilitate the sharing of information between civilian and military organizations, to capture lessons learned and

best practices, and to provide a common knowledge base for the responding civil-military community of interest.

There are numerous and diverse participants on the crisis operations landscape (Figure 1). Typically, the participants "on the ground" and those supporting them can consist of organizations and teams representing the following (reference 3):

- US government civilian and military elements
- Multinational civil-military partners
- International Organizations (IOs)
- Inter-Governmental Organizations (IGOs)
- Non-Governmental Organizations (NGOs)
- Contractors
- Business community (including private military corps)
- Affected nation government and population
- Media (local, regional and international)

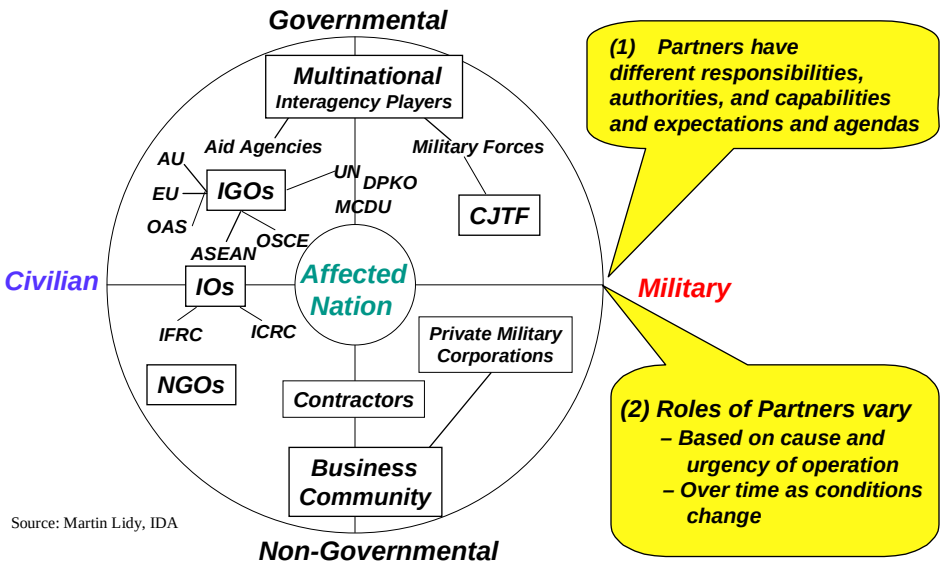


Figure 1. Potential Global Partners During S&R Operations

The diversity of the responding organizations and teams is, in many ways, a real asset. It allows different organizations to bring to the table complementary capabilities, resources and expertise. But the various groups also bring with them different agendas, operating principles, sensitivities, expectations, accountability mechanisms, ICT capabilities, experiences, skills, and lines of authority. Often, military and civilian authorities have little control over many of the participants.

Setting the Stage

Identifying information and information sharing needs is not easy. Natural disaster humanitarian assistance and S&R operations are, by their very nature, complex and dynamic situations. They are multi-sectoral and multi-disciplinary, incorporating both the physical and social sciences. Information is constantly changing, comes from a multitude of sources and is often incomplete or contradictory. In some cases, there is an overload of information and, in other cases there are complete gaps in what is known. Collecting situation awareness information is often difficult, if not impossible, because of inaccessibility to the affected areas due to natural hazards, lack of a safe and secure environment or government restrictions. There is also a certain amount of misinformation and disinformation generated about crises. Common terms used by the military and civilians often have different meanings. For example, the term sector means a geographic area of responsibility for a military organization while it is a functional area such as water/sanitation, food, or shelter for the humanitarian and civilian reconstruction and development organizations.

Another challenge is the inconsistent use of standardized meta-data when collecting and providing crisis operations information. All incoming and outgoing data and information should include the source and the date or time-stamp, so that other users can determine the credibility and currency of the content. Likewise, it is important to make sure that ambiguous terminology is clearly defined and methodologies and indicators explained, so that others can use the data and information correctly. Finally, data and information should be geo-referenced to include information such as the latitude/longitude, geo-code, gazetteer place name and administrative unit so that the data can be entered into a Geographic Information System (GIS) and mapped. If these standards are followed, data and information provided by many different civil-military organizations can be effectively pooled, compared, contrasted, validated and used for analysis, mapping and operational activities.

The information needed by each civilian and military organization and team differs according to its mission, the situation on the ground, the needs of the population in the afflicted zone, the decisions of the affected-nation government, and the phase of the response. For example, organization policy makers want “big picture snapshot” analysis in order to understand the issues, to make decisions on providing assistance, and to be alerted to problems and obstacles. Field personnel and project and desk officers in crisis response organizations, on the other hand, need more detailed operational and programmatic information in order to plan and implement humanitarian assistance and reconstruction programs. Crisis response operations are a highly dynamic information environment. Informational needs can change by the hour--sometimes by the minute. Collaboration does happen, but often in an unplanned, unrehearsed way. Crisis operations are necessarily messy and *ad hoc*, but the result is often a general lack of mutual understanding of roles, relationships and capabilities. Not surprisingly, this contributes to a problematic lack of communication and information sharing among the civilian and military elements of groups that are operating side by side.

Experiences and lessons from recent real-world relief efforts and post-conflict recovery operations also suggest the need to create a common culture of trust in information networks and communications between civilian government elements, military organizations, IOs and NGOs. Communications must flow in all directions, all the time. Information structures need to be flexible (but not *ad hoc*). Finally, "lessons learned" need to be understood after events occur, and the required improvements must be institutionalized. All of this must happen in the context of multiple levels of interaction (reference 4):

- Within organizations (including "reach-back" to home offices);
- Between organizations (bilaterally);
- Among organizations (multilaterally, as in a networked community);
- With local leaders and decision-makers;
- With the media;
- Among the parties in any ongoing conflict; and perhaps most importantly,
- With the local population.

As noted in the Introduction, the absence of "trust" is a fundamental source of tension among the civilian and military participants, as well as the local population and elites. Therefore, the key to success and relationship-building among individuals and organizations lies in understanding the roles, relationships, capabilities, motivations and information-sharing needs in this complex environment. It is also vital to manage expectations and to ensure that all actions support these expectations.

Current ICT Baseline

It is a reasonable assumption that the telecommunications infrastructure of the country in which a crisis operation takes place has been damaged. It may no longer have (if, indeed, it ever did have) sufficient surge capacity, bandwidth or coverage to support the operational needs of all participants in a relief or reconstruction effort. Assisting militaries, civilian agencies, IGOs, IOs and NGOs often bring their own capabilities to augment those of the remaining local telecommunications. For example, modular, packaged systems are often flown in to replace the damaged or destroyed commercial networks. In some cases, commercial "cellular on wheels" (COWs) networks, transportable transmission systems and Wireless Fidelity (WiFi) "hot spots" are deployed, providing additional capacity and coverage.

Commercial satellite systems are used for voice communications and remote access to the Internet. Satellite systems such as the International Maritime Satellite (INMARSAT), Iridium, Thuraya and Globalstar provide voice and limited data service from small, often handheld, terminals. For larger data flows, Very Small Aperture Terminal (VSAT) satellite links and networks are set up to support temporary fixed-installation needs, such as information and coordination centers. INMARSAT Mini-M, Broadband Global Area Network (BGAN) and Regional Broadband Global Area Network (RBGAN) satellite terminals are used to establish remote satellite access to telephone and Internet service.

The emergence of the Internet in the last ten years has revolutionized the availability and dissemination of crisis related information. E-mail and Web portals and surfing have greatly facilitated the transmission of information between the headquarters of the crisis response organizations and the personnel, teams, and programs located in the affected countries. The Internet provides a vast, virtual library of information to users with access.

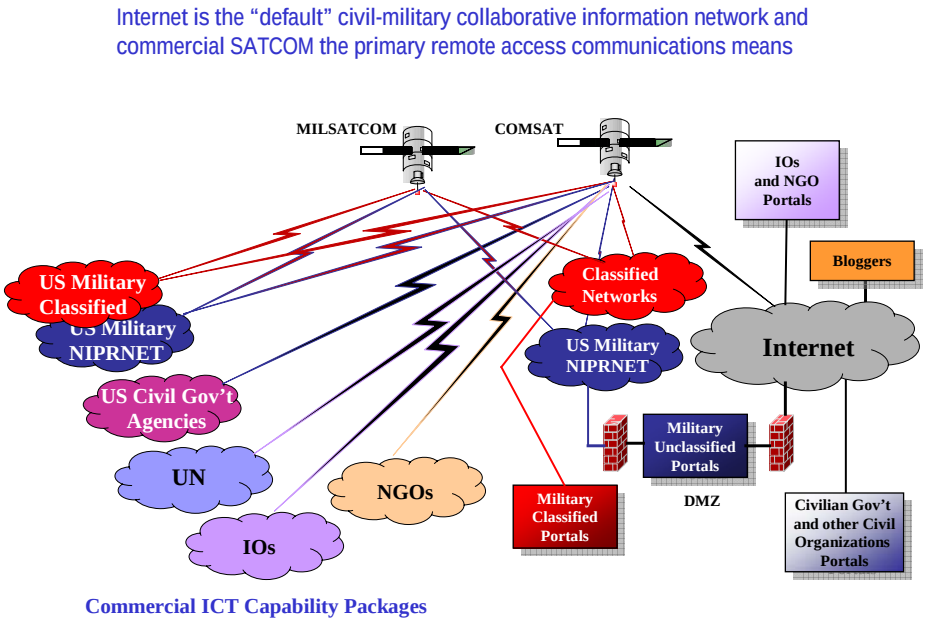


Figure 2. Civil-Military S&R ICT Responses

Commercial ICT capabilities are becoming more pervasive with each new crisis operation (see Figure 2). Civilian and military elements deploy with laptops, cell phones and, often, satellite phones. They use "personal digital assistants" (PDAs), handheld sports radios, and High Frequency (HF), Very High Frequency (VHF), and Ultra High Frequency (UHF) radios to communicate. Ground-to-air radios are used to coordinate air operations such as helicopter transportation for emergency supplies and relief personnel. Land mobile radios are used for emergency service communications. To the extent possible, participants also use the public switched telephone systems and cellular networks to communicate and access the Internet through local Internet Service Providers (ISPs) -- if they exist in the affected area. Cell phone text messaging is used as well. Global Positioning System (GPS) receivers are used not only for location identification and navigation but also to geo-reference data collected in the field. GIS and mapping tools are used for assessments and visualization of situation awareness. Collaboration software tools such as NetMeeting, Groove, SharePoint and InformationWorkSpace (IWS) are used to create shared workspaces online. Terminals with these tools are linked by wireless or wired Local Area Networks (LANs) which are then linked to the Internet via commercial satellite access or other means. Along with other tools and Internet access, collaboration tools can help enable responders to make the most productive use of

e-mail, Web surfing, limited data exchange and video conferencing. Voice over IP (VOIP) applications, such as Skype, are used for voice communication via the Internet and other IP managed networks.

The larger civil-military elements responding to a complex emergency will bring with them the necessary ICT to support their mission needs. The military will respond by implementing both classified and unclassified networks to support their command and control, intelligence, logistics, civil military operations, and other operations and information sharing needs. Military access to the Internet will be provided and Web portals related to the emergency will appear on both the classified and unclassified networks. The large civilian organizations, such as the UN, deploy a significant commercial ICT infrastructure as well to support their assistance operations and information sharing needs. They too create Web portals to share information such as situation awareness, maps, GIS products and other assistance related information. Other civilian organizations deploy with a lesser ICT capability but they also access the Internet where possible and create Web sites to share information. Furthermore, Web logs or Blogs now populate the Internet with information on the crisis.

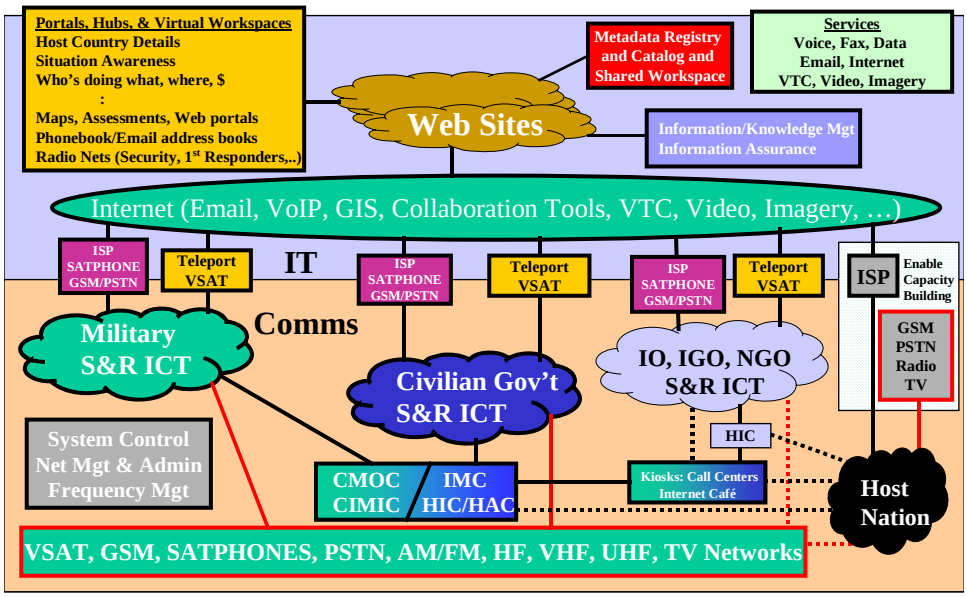


Figure 3. Deployable ICT and Collaborative Information Environment Architecture

Commercial satellites today can provide reasonable cost connectivity to virtually any place on Earth. As a result, they have become a key enabler for extending ICT services to remote, devastated or disadvantaged areas in support of HADR and S&R operations. Portable, mobile and fixed terminals communicate with land earth stations (referred to as "hubs" and "teleports") that interface with the public network for access to voice and Internet services, including e-mail, Web surfing and the use of Web portals. These satellite technologies can be used, in combination with terrestrial networks, to serve as the medium for civil-military coordination. Figure 3 illustrates what could be

referred to as the “default” civil-military ICT and collaborative information environment architecture based on common commercial practices used today.

Shortfalls in the ICT Baseline

In spite of improved use of commercial ICT, the world community response to the Tsunami, Katrina and other recent crisis operations, such as, Afghanistan and Iraq, repeated many of the disjointed approaches to crisis response assistance that have been experienced in the past, particularly with respect to data/information management. Although the need for data and information on these events (for assessing damage, planning relief and recovery efforts, delivering aid) was immense and immediate, the community's response was once again slow and disorganized and somewhat uncoordinated. Repeatedly, the response community found itself unprepared to deal with some of the largest issues of information management (e.g., the ability to locate and acquire data quickly, determine its freshness and share it with others). Information overload and lack of adequate discovery tools were problems as well. These issues hampered or delayed the ability of people on the ground to find and those supporting them to generate the necessary information products for the people who are executing operational activities.

Many of the same issues that have plagued the civil-military response community in past events were once again experienced:

- Very limited “shared informational awareness” to enable everyone to understand what data/information are/will be available, what has been or needs to be done to it, who needs it, or who has it;
- Multiple organizations producing the same information products;
- Organizational use of obsolete data (i.e., “stale” data);
- Stove-piped and incompatible systems that were unable to share information with others because of either format or bandwidth/connectivity issues related to operating in austere ICT environments;
- Numerous applications were incompatible with data/information formats of others;
- Pushing large amounts of data to multiple locations, multiple times;
- End users who’s access bandwidth could not support downloading large data files such as maps;
- Hard for those on the ground to find needed information (i.e., lack of understanding of what was available and how to access, information overload).

There are emerging challenges with deployable ICT capabilities that can have unintended consequences when used by IOs and NGOs operating in non-secure environments. In today's more hostile environment, INMARSAT phones and radio antennas on vehicles can make these elements a target for criminal and terror attacks. Reliance on cellular and satellite phones can also contribute to eroding the use of the traditional line-of-sight secure radio networks that are still employed and used for emergency response communications by organizations such as the UN and its dealings with civilian participants in harm's way.

Although commercial satellite capabilities provide wide-area, spot and global access, coverage and capacity in any particular location can sometimes be limited, especially in remote areas. Responders should therefore not expect wideband services when they begin operations. Low bandwidth, intermittent coverage and overloaded civil telecommunications and satellite infrastructures -- which are not designed to absorb the surge in demand from responders – can significantly degrade end-user performance. Availability of commercial power and ICT repair facilities can be a problem as well. Therefore, it is important to deploy with stand alone alternative power sources, fuel supplies, and spare parts for maintenance. These limitations need to be anticipated and planned for before deploying into a crisis area.

The Internet has added to the overload of information and the increasing difficulty in locating, extracting and verifying the answers to the critical questions—information and knowledge management. There are also Information Assurance challenges—trust and self-policing of information on the network is the norm. No one organization element is responsible for assuring the quality and integrity of information placed on the network and no standards are employed for collecting and populating the various Web sites which adds to the challenges of sharing information

Meanwhile, there is no mutually agreed, global CONOPS or system architecture for ICT support to crisis operations. Furthermore, there is often a lack of leadership in the civil-military community to pull together all of the disparate capabilities and create and manage a federated ICT network and distributed information and knowledge environment. Every deployment is largely an *ad hoc* event that employs "old boy" networks and personal contacts to create workable modes of operation.

The result is a loss of efficiency that often threatens to become a loss of effectiveness – a disturbing prospect in the context of operations that directly lead either to saving, or losing, lives. There are real imperatives to set standards for collaboration, coordination and information sharing. Furthermore, it is critical to identify the technological means to achieve them using ICTs.

Mechanisms to Collaborate and Share Information

Organizational and technical means are used to collaborate and share information. In situations where the military recognizes the need to collaborate and share unclassified

(but sensitive) information with humanitarian and other civilian actors, this will normally be done via a c*ivil-military operations center* (CMOC) or, in NATO parlance, a c*ivil-military cooperation center* (CIMIC). Other collaboration and information-sharing avenues may include the dispatching of military liaison officers to meetings, electronic bulletin boards, Internet Web sites/portals or even simple exchanges of e-mails. Civilian elements establish collaboration (cooperation) and information sharing centers such as the United Nations (UN) Office for the Coordination of Humanitarian Affairs (OCHA) Humanitarian Information Center (HIC) and On-Site Operations Coordination Center (OSOCC) and the US Department of State's Humanitarian Assistance and Coordination Center (HACC) and Information Management Unit (IMU). NGOs and IOs also set up Information Centers (IC). Some centers include Kiosks and Internet Cafes that can be used to provide civil-military responders as well as the broader public access to telephone and Internet services in affected areas.

Creating a common communications culture must be done without undermining either the neutrality of civilian IOs, IGOs and NGOs or the military's safeguarding of operational security information. A list that details who is doing what, where, is useful for resource allocation and management in relief and reconstruction. However, in the wrong hands, it can also be a target list for groups and individuals that want to use violence for political ends. The creation of a *collaborative information environment* (CIE) (see Figure 4), therefore, requires a balance between openness and security. But it can be done only if everyone is sensitive to one another's concerns.

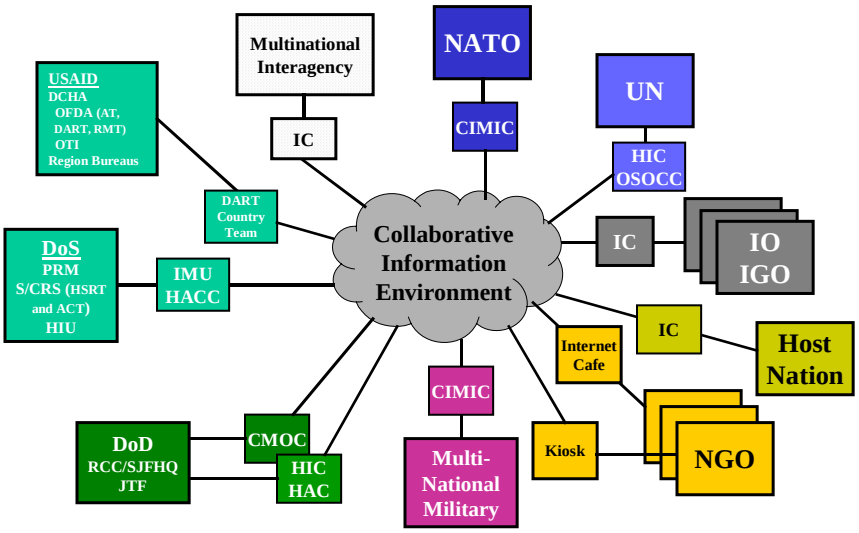


Figure 4. Example of Field Coordination Mechanisms: Organization Means

Perhaps the first step in building a CIE is to cultivate willingness among the civil-military participants to create a common communications culture and to minimize

barriers to participation once established. One can then create mechanisms to collaborate and share information by:

- Using a common ICT response architecture (a federated network) employing the Internet, commercial ICT products and services, Web portals and metadata repositories;
- Creating a suite of interoperable ICT "toolkits";
- Extending ICT capabilities to a crisis area to be shared, as appropriate;
- Facilitating and promoting collaboration and information sharing among participants;
- Supporting the building of affected-nation ICT surge capacity and infrastructure recovery and reconstruction as needed;
- Forming civilian CIO and military J6/G6/C6 or equivalent collaboration arrangements, with needs assessment and requirements, planning and implementation, and federated network management and operations.

The ability to provide a ubiquitous ICT network, with the agility and adaptability for authorized participants to "plug and play" with their own equipment, means the CIE needs to respond effectively to event-driven, high-tempo, short time-scale, uncertain, diverse and dynamically-varying operations. The CIE needs to be able to mediate flexible and timely interaction between "come-as-you-are" heterogeneous systems and information databases. It needs to support agile C2, shared situation awareness, and improved interoperability and collaboration.

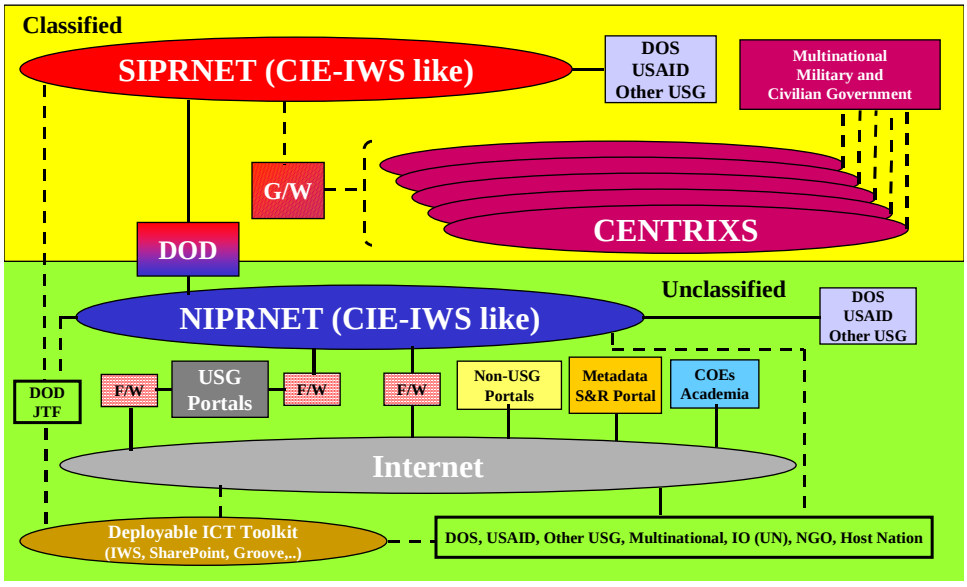


Figure 5. Field Coordination Mechanisms: Technical Means

The technical means used today to facilitate coordination within classified and unclassified information environments (reference 5) are illustrated in Figure 5. The US military's classified and unclassified networks are largely based on employing secure guard gateways and strict Information Assurance (IA) processes to carefully manage and control access and use privileges. On the other hand, the world's largest unclassified network, the Internet, operates in a highly trust-oriented operational environment with little, if any, IA measures.

Military and other agencies that produce classified products need mechanisms that allow them to more easily partition information so that some of it can be routinely released to coalition military partners (at lower classification levels) and non-military parties, such as IOs and NGOs (fully declassified). There is also a need to more effectively deal with multiple levels of classification and the protection of dissemination within those multiple levels. The CIE, therefore, should be able to accommodate the management of access privileges, security, and performance. This has both collection and dissemination aspects in terms of access to, and use of, the CIE.

Language differences continue to challenge operational cooperation, and there is a need for machine-translation tools to help fill the translation gap. As noted, interoperability means not only technical and political compatibility, but also the will and the means to communicate, to cooperate, and to collaborate -- in short, sharing a common culture of communication. When systems are not politically, organizationally, or technically interoperable, information becomes "stove-piped" within a single organization, and systems cannot easily collaborate.

The CIE needs to be able to accommodate a diversity of users, along with the diversity of organizational cultures, equipment, systems and databases they bring with them. There is also a need for improved data collection, decision-making tools, analysis capabilities, and visualization aids that meet the needs of S&R and HADR requirements. Included in this is the need for data and information management strategies that can be used to guide collection management, analysis, and database capabilities. Tools to support predictive assessment and course-of-action planning for S&R operations are needed as well, including Measures of Merit (subsuming Measures of Effectiveness and Measures of Performance) for measuring progress and the success of actions. Finally, the CIE needs to be scalable in terms of number and diversity of the civilian and military users. Moreover, it must be easily and rapidly deployable into the area of operations and able to accommodate that environment. This may call for stand-alone capabilities including a power supply and operations and maintenance support.

The creation of a collaborative military and civilian computing and communications environment is achievable with today's technology. An approach to creating a civil-military CIE is illustrated in Figure 6 and is based on the following assumptions:

- The Internet, satellite links and cellular phones will be the preferred media for communicating and sharing information among the civil-military participants.

- Commercial satellite service will likely be a primary means of gaining access from remote areas and to the Internet.

- A common suite of ICT capabilities (e.g., a "toolbox" containing cell phones, radios, satellite phones, VSATs, PDAs, laptops, workstations, WiFi networks, collaboration tools, GPS receivers, GIS products) can be selectively packaged and tailored to meet the anticipated ICT operational support needs.

The civilian and military responders will in some cases do the satellite access systems engineering, acquisition and integration themselves. That is, they will determine what they need and then purchase or lease VSAT terminals, satellite phones, hubs, teleports and satellite access, make the necessary Internet access arrangements and set up and manage their own networks. Or, they will engage a satellite service provider and/or a systems integrator to do all this for them. Responders can take advantage of emerging NGOs and private companies that are now offering turnkey or managed satellite and Internet access services. Some packages may include the set-up and management of an information center in the operations area.

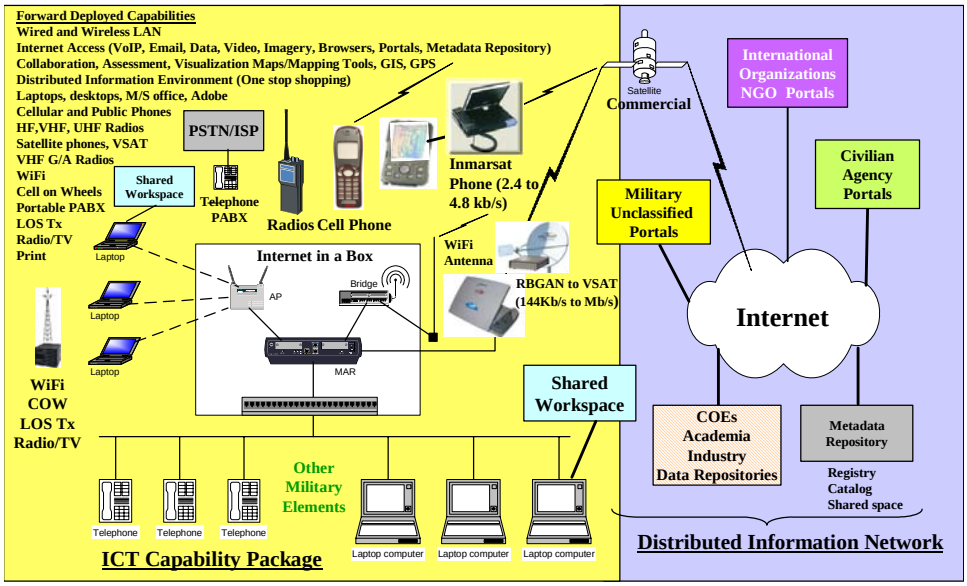


Figure 6. Commercial ICT Capability Packages and Collaboration and Information Sharing Arrangements

Adequate consideration must be given to local government regulations governing the use of equipment and frequency assignments for satellite, radio and wireless networks. Proper cellular phone, radio, WiFi and satellite access configurations are vital. It is important to have local government approval for their usage, along with service agreements with satellite, telephone, Internet access and teleport service providers before deploying ICT capabilities forward.

Common practice for many civilian and military entities today is to create Internet portals and metadata repositories in an effort to provide a "one-stop-shopping" capability for access to information about the crisis situation. Collaboration tool bridges will likely be needed to facilitate exchanges among different collaboration tool suites (e.g., IWS and Groove).

Presumably, the responder community will employ smart systems engineering practices to create appropriate local radio (HF, VHF, UHF) and cellular networks to facilitate communications among responders on the ground. Furthermore, agreements will be needed for data standards and smart management of the information that will populate the various Web portals created to support the response operation. This should include the creation of a metadata repository to facilitate information discovery.

Regarding data, Data Sharing in a Net-Centric Department of Defense, DoDD 8320.2 (reference 6) identifies a set of seven goals to make data more readily available and usable. For each of those seven goals they have identified a set of actions to achieve those goals. Although these goals and actions are generic, they can be tailored to meet the needs of the crisis response community.

- The first of these goals is to make data visible. This is to be achieved by posting data to shared spaces, associating discovery metadata with data assets, creating and maintaining catalogs; registering metadata related to structure and definition, and inventorying data assets.

- The second goal is to make data accessible. It is recommended that this be implemented by creating shared spaces and data access services and developing associated security-related metadata.

- The third goal is to institutionalize data management. To do so requires that the community govern data processes with sustained leadership; incorporate data approaches into Community of Interest (COI) processes and practices; advocate, train, and educate in data practices; and adopt metrics and incentives.

- The fourth goal is to enable data to be understandable. This can be accomplished by defining appropriate ontologies and metadata. The latter should subsume both content- and format-related metadata.

- The fifth goal is to enable data to be trusted. To approach this issue, it is necessary to associate data pedigree and security metadata, and to identify authoritative sources.

- The sixth goal is to support data interoperability. A set of four steps are envisioned to realize that goal. These include registering metadata, associating format-related metadata, identifying key interfaces between systems, and complying with net-centric interface standards.

- The final goal is to be responsive to user needs. This implies involving users in COI and establishing a process to enable user feedback

IA will need to be more than "trust" and self-discipline by the user community. Appropriate security measures are required to protect and restrict unauthorized access to unclassified but operationally sensitive information. The community will need to have agreed mechanisms in place to ensure the quality and integrity of information populating the Web sites and to coordinate management of the resulting federated information network. Finally, appropriate network security and IA protection must be implemented to protect against intrusions, viruses, malicious code and misuse of the network information.

Best Practices

The attempt to assemble "best practices" is an effort to distill clear guidelines from the real-world experiences of professionals who have already faced the inevitable challenges – and overcome them. Best practice statements are the record of how those challenges were minimized and resolved. They can then be published and disseminated as "trail markers" to make sure those who follow in their footsteps can avoid pitfalls. The best practices incorporated in the Primer were derived from multiple sources, such as the UN, the U.S. DoD and DOS, USAID, industry, professional workshops, NGO organizations, and other subject-matter expert sources. The best practices address a range of subjects such as implementing civil-military coordination and information sharing; establishing a CIE; dealing with data and information; preparing for deployment; and conducting operations. Some examples follow:

Civilian-Military Coordination

- Understand the other participants
- Respect their legitimate limitations
- Pay special attention to geographic and sectoral boundaries
- Leverage the shared interests of participants
- Build and carefully use networks
- Take the initiative in information sharing
- Have multiple, simple, reliable means of sharing information
- Encourage training and preparation for task sharing
- Provide the tools to facilitate joint planning

- Avoid public criticism of any participants

Civil-Military Information Sharing

- Social and organizational issues
    - Ensure that all reports compiled by responders have clear time and date stamps.
    - Be sure to confirm which metrics are being used and try to establish uniformity among responders.
    - Establish the variations in meaning for terms used by providers and, wherever possible, be conscious of different usages.
    - Try to avoid depending on the military for data that are time-sensitive and has not been shared before. State the information need in terms of the decision that must be made rather than the raw data that is being used to make the decision.
    - It is important to know how data was collected, and by whom, in order to judge whether it may be valuable or verifiable as a basis for action.
    - Pay attention to the effects of institutional cultures, as well as the informational and ethnic cultures of the affected countries.
    - Remember that when the military reacts to an emergency, one of the first things they will do is restrict access to their critical facilities such as their operations center. The civilian elements must know how to gain access in these emergencies and must make these arrangements before the emergency.

- Technical issues
    - Before sharing facilities, weigh cost savings and expedience against the possibility that services will be disrupted if someone decides to target military communications infrastructure.
    - If military forces have the technical capability and are willing to evaluate or repair communications or computer systems, this may be an area of low-visibility, indirect assistance that could benefit the humanitarian community.
    - At a minimum, a memorandum of understanding should be negotiated to ensure equitable access to radio frequencies and satellite resources.

- Partnerships
    - Maximize resources by establishing partnerships with participants in S&R and HADR operations
    - Engage local and national actors in information projects and develop networks of local communities and national NGOs, civil society groups and the private sector, to decrease dependency.

- Promote trust and transparency through IT linkages.
- Partner with the media as an effective way of communicating information to the affected population.

Establishing a CIE

- Conduct an assessment of information needs and existing knowledge resources in advance, and identify the gaps in data, information and knowledge.

- Provide standardized meta-data (source, date, geo-reference, definitions) along with all collected and shared information, so that it can be pooled, compared, verified, mapped, and used for analysis.

- Establish and use collaboration networks to create COIs among individuals in multiple organizations as a means to capture and share tacit knowledge and dismantle organizational stovepipes.

- Employ visualization to represent complex data and information, display patterns and relationships, and depict a geo-spatial common operating picture.

- Demonstrate the practical applications of new information tools and technologies and use collected data and information to answer questions and respond to identified information needs.

- Recognize the value of tacit knowledge gained from field experience, collaboration and learned expertise.

Data and Information

- Ensure data are visible, available, and usable when needed and where needed to accelerate decision-making.

- "Tag" all data with metadata to enable discovery of data by users.

- Post all data to shared spaces to provide access to all users except when limited by security, policy, or regulations.

- Advance the COI from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of a net-centric data environment.

Preparing for an Operation

- Maintain preparedness "toolboxes" for online and offline distribution.

- Develop surge capacities for rapid deployment.

- Preserve institutional operational memory.

- Develop contact lists (e.g., lists should feature key humanitarian responders and local personnel, with phone numbers and e-mail addresses).

- Review affected-nation legal, regulatory and institutional considerations.

- Obtain the affected government's permission to import and operate communication equipment within and across borders.

- Define an exit strategy.

Conducting an Operation

- Know how to get in contact with the right people in the most expeditious and appropriate manner to facilitate resolution of civil military issues.

- Share information, to the extent feasible, since no single organization has all of the data, information, and knowledge about crisis operations.

- Use unclassified, open sourced platforms and channels for unclassified information, to the extent feasible.

- Establish a formal process for the humanitarian community to request information from the military forces.

- Create a common relevant, releasable operational picture that can be used by all.

- Collect, organize, and disseminate information in a manner that will benefit the population and polity of the affected country.

Summary

There is a broad consensus that ICTs are necessary enablers for the smooth, effective operation of HADR and S&R operations. Moreover, a growing number of participants in these operations – from military units to the smallest NGOs – are bringing at least some elements of their ICT capabilities with them when they deploy. Yet, the watershed events of recent years (e.g., the Indian Ocean tsunami, the rash of Caribbean hurricanes and devastating earthquakes in Iran and Pakistan) illustrate there is no default or standardized suite of equipment, databases and operational protocols to follow when these organizations attempt to work together for humanitarian, reconstruction or development purposes.

This paper has addressed ICT for civil-military coordination in crises. It included a description of the current ICT baseline, its shortfalls and options to mitigate these

shortfalls. It presented examples of best practices developed from experience. The practices addressed civil-military information sharing, the challenges in establishing a CIE, a strategy for collecting data, managing information, and seeking knowledge and the steps to take in preparing for, and conducting, an operation. The Primer is a "living document" that will be refined as we continue to develop insights from real world crises.

References

1. "Transforming for Stabilization and Reconstruction Operations", Hans Binnendijk and Stuart Johnson, National Defense University, 2004.
2. DoD Directive 3000.05, Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations, 28 November 2005.
3. Miscellaneous HADR and S&R related briefing material, Martin Lidy, IDA, 2005
4. "Creating a Common Communications Culture", USIP, Virtual Diplomacy Initiative, 2004
5. DoD Instruction 8110.1, Multinational Information Sharing Networks Implementation, 6 February 2004.
6. DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense, 2 December 2004.

Perspectives on Information and Communications Technology (ICT) for Civil-Military Coordination in Crisis

Gerard Christman
Office of the Assistant Secretary of Defense for
Networks and Information Integration (OASD(NII)),
Directorate for Contingency Support and Migration Planning (CSMP)
Franklin Kramer, Stuart Starr, Larry Wentz
National Defense University (NDU), Center for Technology and National Security Policy (CTNSP)

2006 CCRTS

Agenda

- Introduction
  - Crisis operations landscape
  - Context
- Primer snapshot
  - Nature of the challenge
  - Current knowledge of ICT
  - Best practice example
- Summary

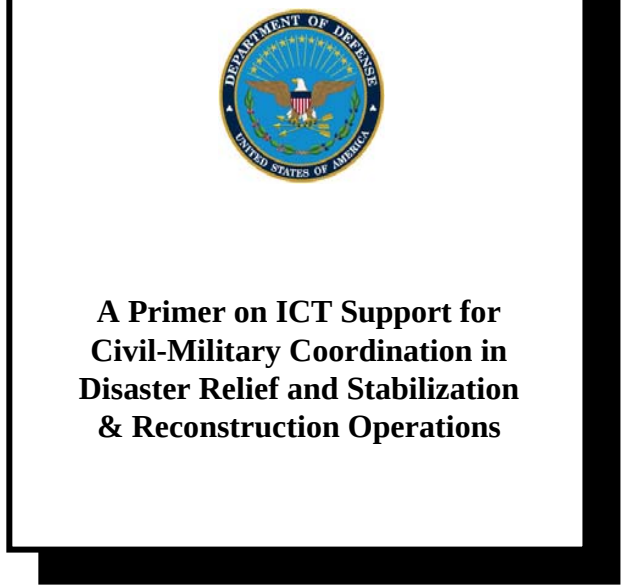
Crisis Operations Landscape

- Categories of crises
  - Humanitarian assistance and disaster relief (HADR)
  - Stabilization and Reconstruction (S&R) operations
  - Complex emergencies
- Diverse civilian and military participants and capabilities
  - Mix of military, civilian government, International Organizations (IOs), Nongovernmental Organizations (NGOs), contractors, media, and local population and leaders
    - Military and/or civilian authorities have little control over many of the participants
    - At best, limited unity of effort
  - Differing responsibilities, agendas, experiences, expectations, accountability, and understanding of each others roles and capabilities
  - Wide range of ICT capabilities and “stove-piped” deployments
  - Civil-military collaboration and information sharing problematic

Context

- Types of crises can differ in their causes and specific impacts, but… *there are significant **similarities** in the information and ICT support needed to enable each of them*
- Partnership established between CSMP, OASD(NII) and CTNSP, NDU, in conjunction with military, civilian government, IO, and NGO elements, to identify
  - Common civil-military information needs
  - Current commercial ICT state of the practice supporting recent crisis operations
- Major product from partnership
  - A Primer on ICT Support for Civil-Military Coordination in Disaster Relief and S&R Operations
  - Designed to identify current knowledge and best practices

ICT Primer Snapshot



PART ONE – The Nature Of The Challenge

- Participants in Civil-Military Coordination
- Information Needs
- Civil-Military Cultures and Challenges
- Guiding Principles

PART TWO – Tool Kits And Best Practices

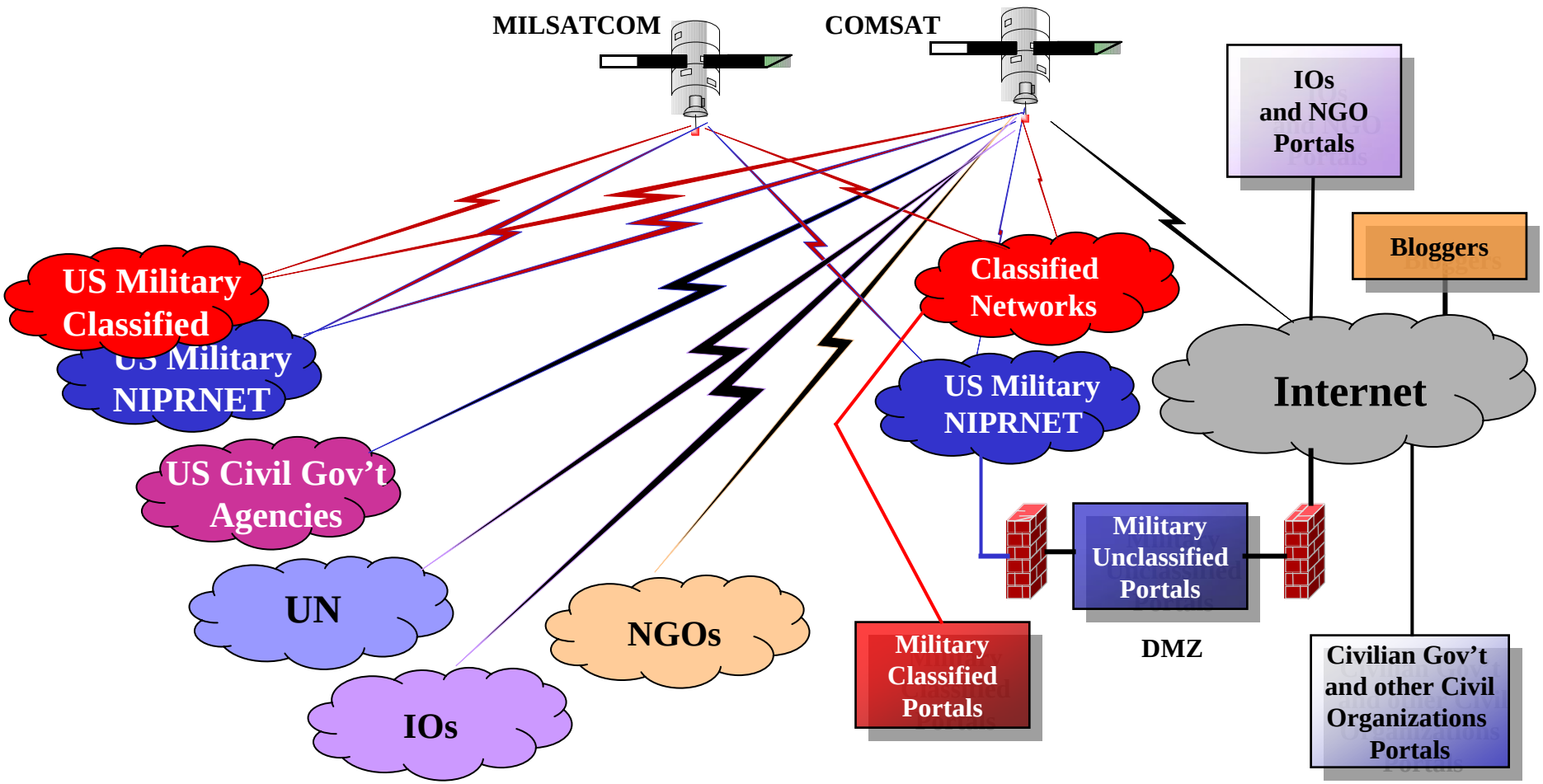
- ICT Toolkits
- Data and Information Management
- Best Practices
- Trends in the Use of Commercial ICTs

Nature of the Challenge

- No single responding entity can be the source of all the necessary information -- operationally there is the need to share
- Responding civil-military elements bring their own ICT
  - Lack agreed ICT strategy, CONOPS, and architecture
  - Some with lesser capabilities than others
  - However, common commercial ICT capabilities becoming more pervasive
- There are several civil-military collaboration and information sharing issues
  - Information sharing versus intelligence gathering
  - Military classification (e.g., operations security) versus civilian need for transparency
  - Trust building and shared use of commercial ICT as enablers
- Furthermore, there are issues with cultural awareness and language; e.g.,
  - Responding organizations and participants
  - Affected nation (including information culture)

Civil-Military ICT Baseline

Internet is the "default" civil-military collaborative information network and commercial SATCOM the primary remote access communications means



Commercial ICT Capability Packages

Shortfalls in the ICT Baseline (1 of 2)

- Very limited “shared informational awareness” to enable everyone to understand
  - What data/information are/will be available
  - What has been or needs to be done to it
  - Who needs it, or
  - Who has it
- Multiple organizations producing the same information products
- Organizational use of obsolete data (i.e., “stale” data)
- Stove-piped and incompatible systems that were unable to share information when operating in austere ICT environments because of issues in
  - Format or
  - Bandwidth/connectivity

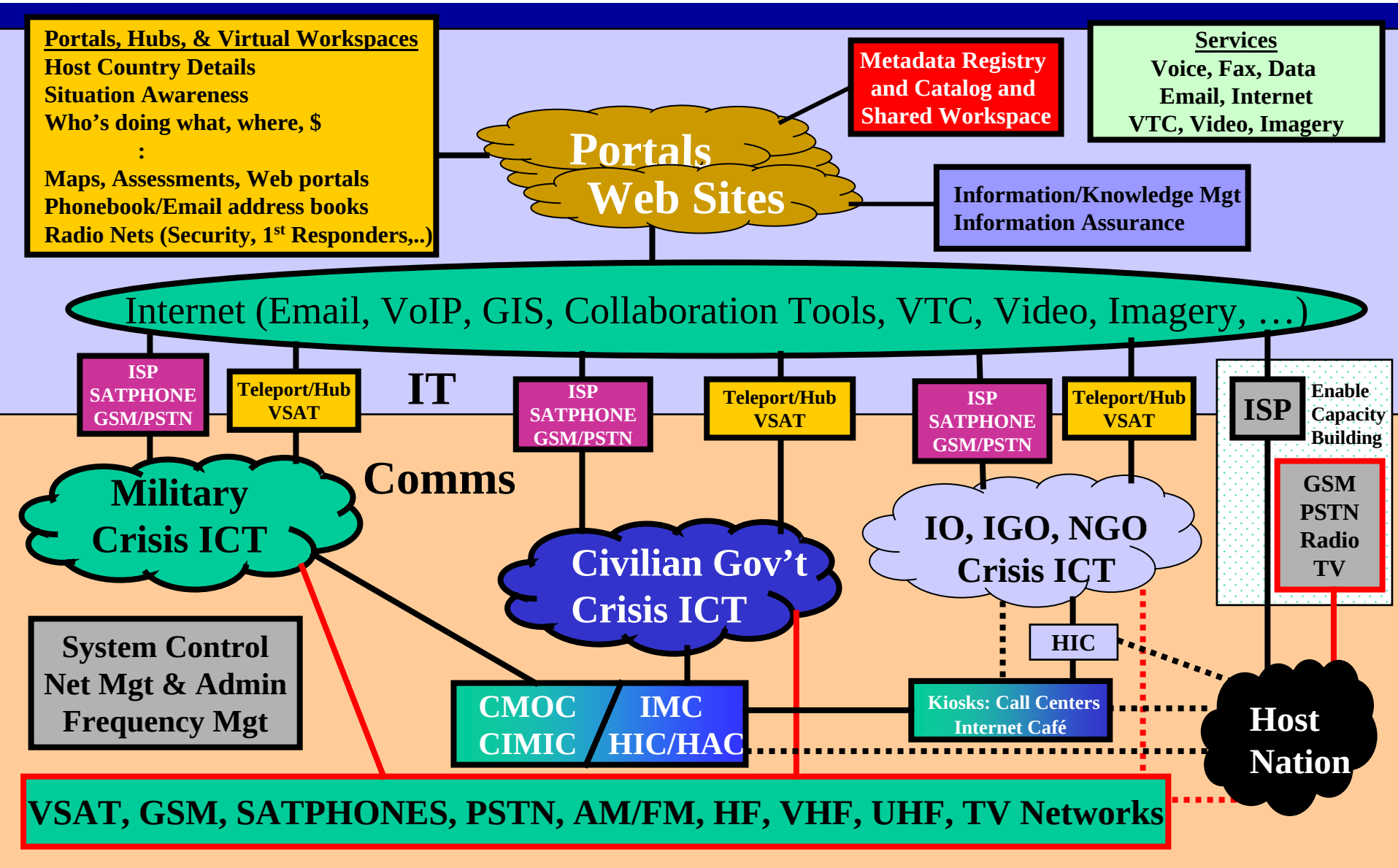
Shortfalls in the ICT Baseline (2 of 2)

- Numerous applications were incompatible with data/information formats of others
- Pushing large amounts of data to multiple locations, multiple times
- End users who's access bandwidth could not support downloading large data files (e.g., maps)
- Difficult for those on the ground to find needed information; e.g.,
  - Lack of understanding of what was available and how to access
  - Information overload

Options to Mitigate Shortfalls

- Use a common ICT response architecture employing
  - The Internet, WiFi, cellular, and satellite as preferred media
  - Commercial satellite service as primary access from remote area
  - Commercial ICT products and services
  - Web portals
  - Metadata repositories
  - Network administration and management
  - Information assurance and knowledge management
- Create a suite of interoperable ICT “toolkits”
- Agree on data sharing goals and actions to ensure data are visible, available, usable when needed and where needed, and “tagged” and geo-referenced to enable discovery

Common ICT Response Architecture



Interoperable ICT "Toolkits"

Forward Deployed Capabilities
Wired and Wireless LAN
Internet Access (VoIP, Email, Data, Video, Imagery, Browsers, Portals, Metadata Repository)
Collaboration, Assessment, Visualization Maps/Mapping Tools, GIS, GPS
Distributed Information Environment (One stop shopping)
Laptops, desktops, M/S office, Adobe
Cellular and Public Phones
HF,VHF, UHF Radios
Satellite phones, VSAT
VHF G/A Radios
WiFi
Cell on Wheels
Portable PABX
LOS Tx
Radio/TV
Print

PSTN/ISP

Shared Workspace

Telephone PABX

Radios Cell Phone

Inmarsat Phone (2.4 to 4.8 kb/s)

Satellite

Commercial

International Organizations NGO Portals

Civilian Agency Portals

Military Unclassified Portals

WiFi Antenna

RBGAN to VSAT (144Kb/s to Mb/s)

Internet

Laptop

Laptop

Laptop

Internet in a Box

AP

Bridge

MAR

WiFi
COW
LOS Tx
Radio/TV

Shared Workspace

COEs
Academia
Industry
Data Repositories

Metadata Repository

Registry
Catalog
Shared space

Other Military Elements

Telephone

Telephone

Telephone

Laptop computer

Laptop computer

Laptop computer

ICT Capability Package

Distributed Information Network

Best Practice Example: Preparing for an Operation (1 of 2)

- Maintain preparedness “toolboxes” for on-line, off-line distribution
  - Toolboxes provide guidelines and reference tools for the rapid-deployment of ICT packages and/or the establishment of Web sites, intranets and databases under a variety of field conditions
  - Toolboxes should include data standards, operating procedures, training materials, database templates, and manuals
- Develop surge capacities for rapid deployment
  - Maintain rosters of experienced ICT professionals
  - Formulate equipment caches
  - Establish training and exercise programs
- Develop contact lists
  - Lists should feature key humanitarian responders and local personnel, with phone numbers and email addresses

Best Practice Example: Preparing for an Operation (2 of 2)

- Develop cultural awareness and civil-military situation awareness
- Review host-nation ICT related legal, regulatory, and institutional considerations
- Use a rapid response ICT assessment team (2-4 persons) in advance of full deployment to establish needs and conditions on the ground
- Determine communications requirements
- Identify alternative power sources, spares, and repairs
- Setup and test ICT capability packages to be deployed

Summary

- This paper has addressed two major issues
  - ICT for civil-military coordination in crises
    - Baseline
    - Shortfalls
    - Options to mitigate shortfalls
  - Best practices developed from experience
    - Civil-military information sharing
    - Establishing a collaborative information environment
    - Collecting data, managing information, and seeking knowledge
    - Preparing for a deployment
    - Selecting VSAT systems and services
    - Conducting an operation
    - Employing a Web site
- The Primer is a “living document” that will be refined as we continue to develop insights from real world crises